Digital Signatures for the Analogue Radio

Konrad Hofbauer
Graz University of Technology
Austria

konrad.hofbauer@eurocontrol.int

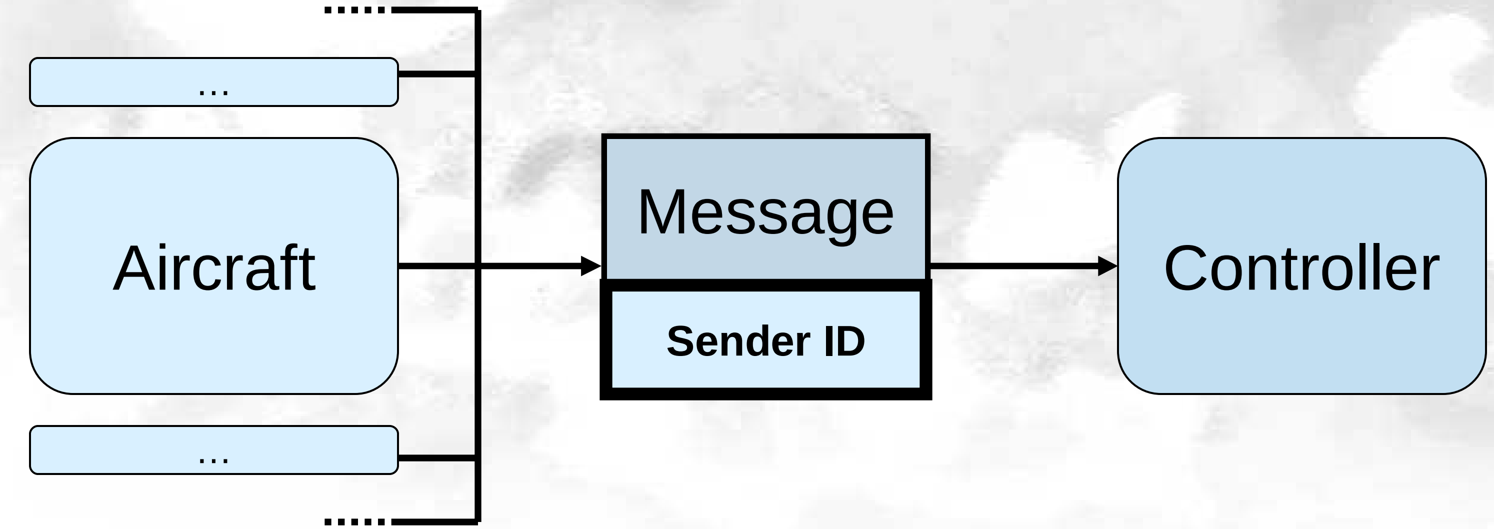
Horst Hering
Eurocontrol Experimental Centre
France

horst.hering@eurocontrol.int

Problem Context

- Communications
  - ➔ Air - Ground
  - ➔ Analogue voice
  - ➔ Legacy VHF radio

- Party line channel
  - ➔ Controller and pilots
  - ➔ Identification
  - ➔ Call sign

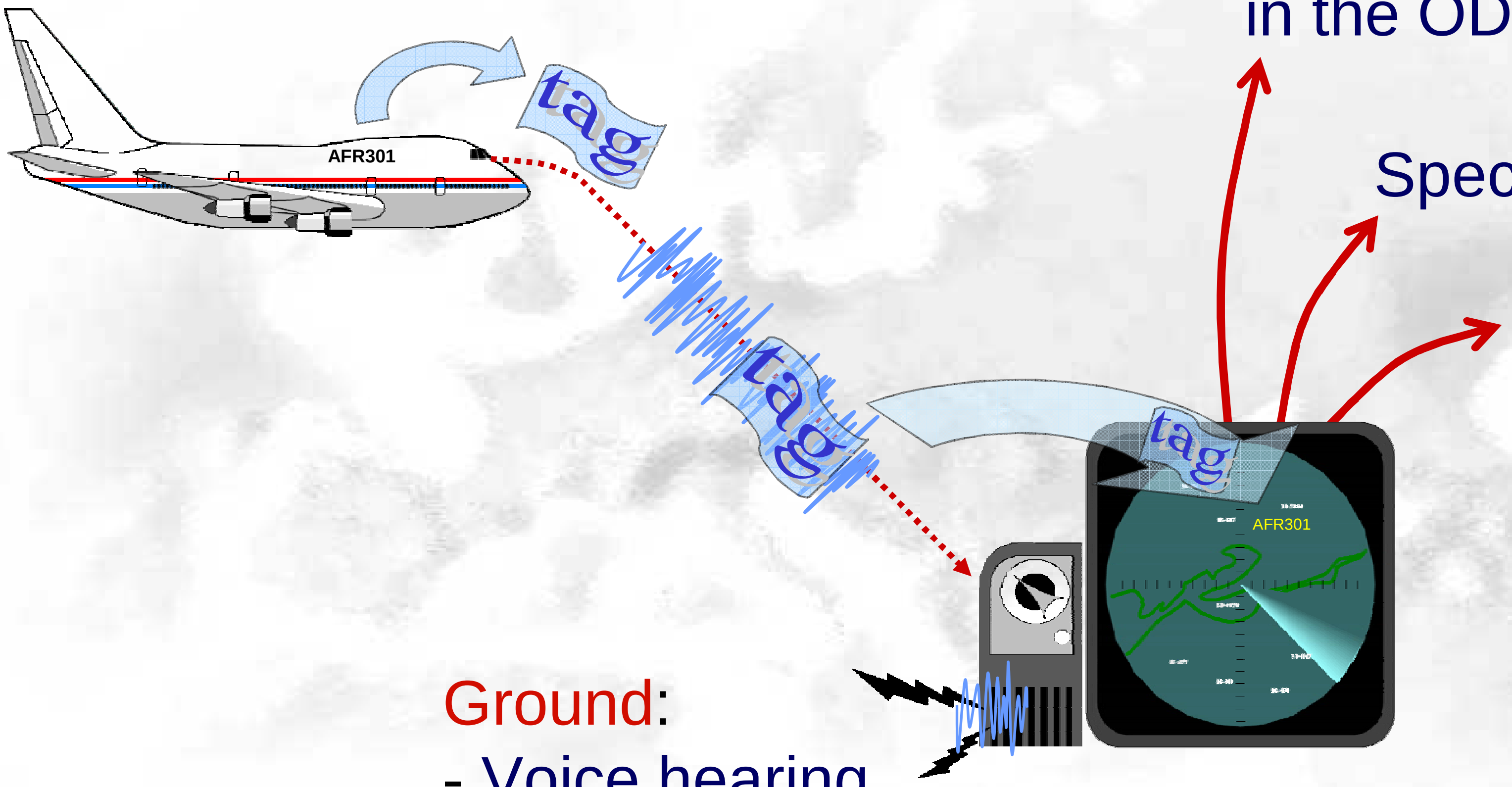


Threats … related to Sender ID

- **Call sign confusion and ambiguity**
  - ➔ “Mis-Identification”
  - ➔Safety Threat
- **Malicious messages**
  - ➔ Radio transmissions issued by unauthorized 3rd party
  - ➔Security Threat

Digital Signature (Tag)

Aircraft
VHF-radio communication:
voice with added tag



Innovative functions in the ODS

Special displays

3D audio

Ground:
- Voice hearing
- Decoding of digital signature

Specifications

Deployment-driven requirements

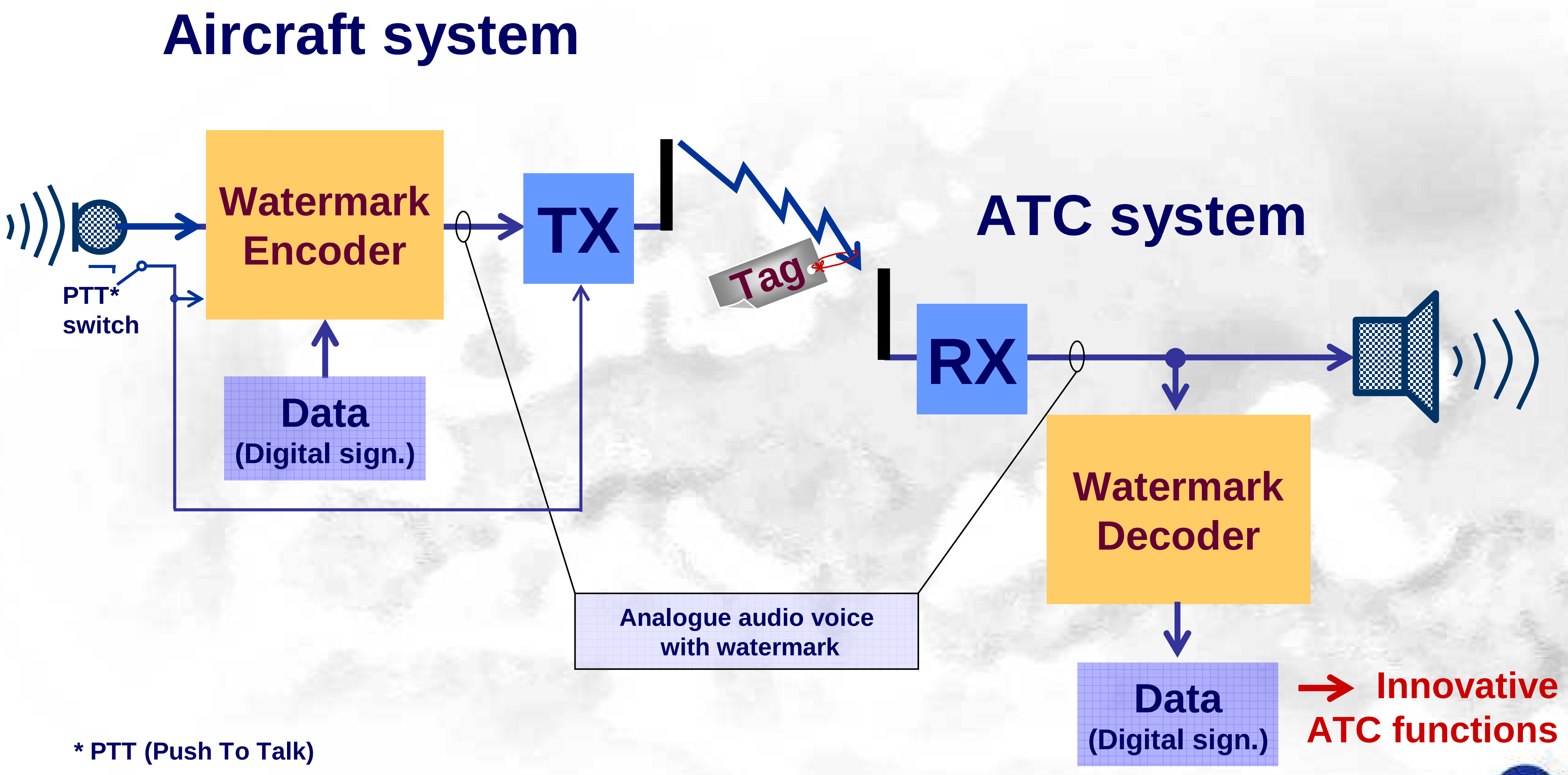
- ➔Rapid and simple deployment
  - ⇨Legacy system compliance
  - ⇨Bandwidth efficiency
  - ⇨Minimal aircraft modifications
  - ⇨Cost efficiency

Specifications

User-driven requirements

- ➔Perceptual quality
- ➔Data rate
- ➔Real-time availability
- ➔Error rate
- ➔Maintaining established procedures
- ➔No user interaction

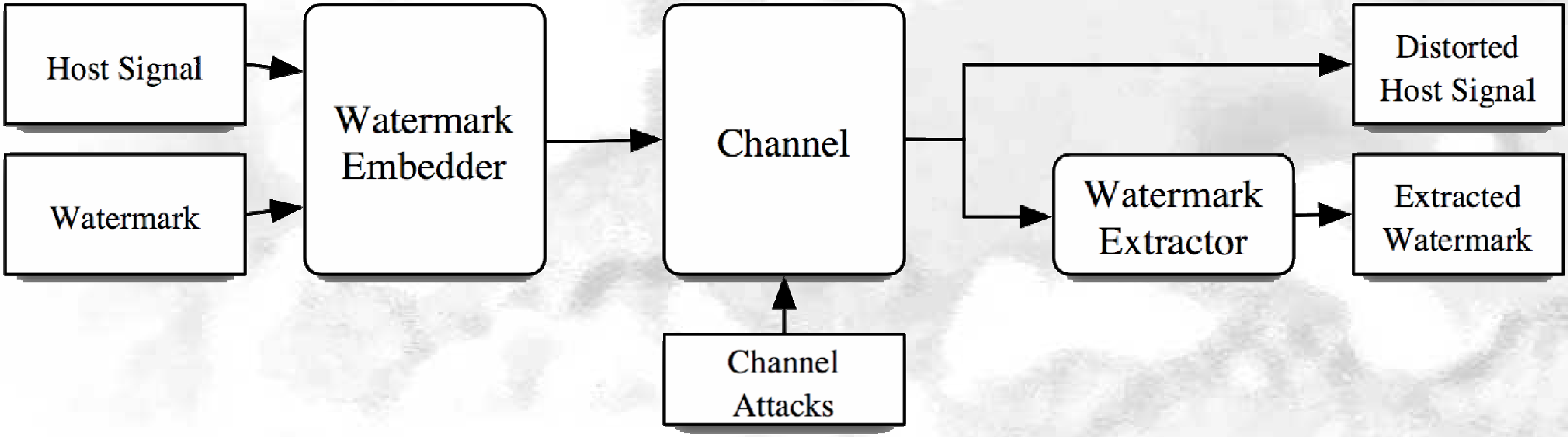
Information Embedding



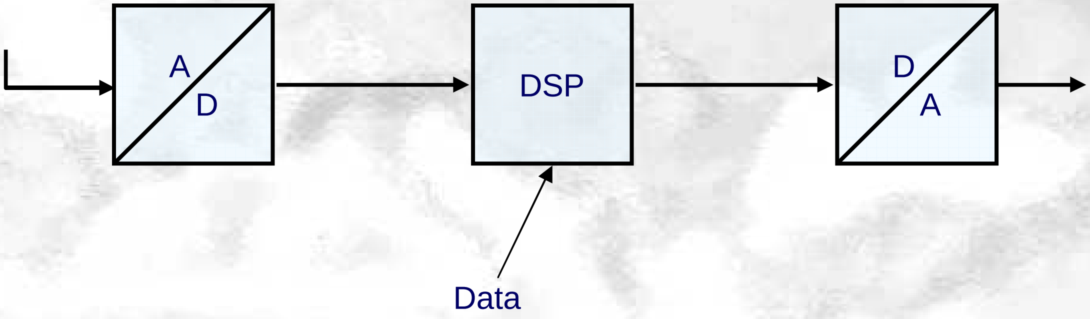
* PTT (Push To Talk)

Digital Watermarking

System Model

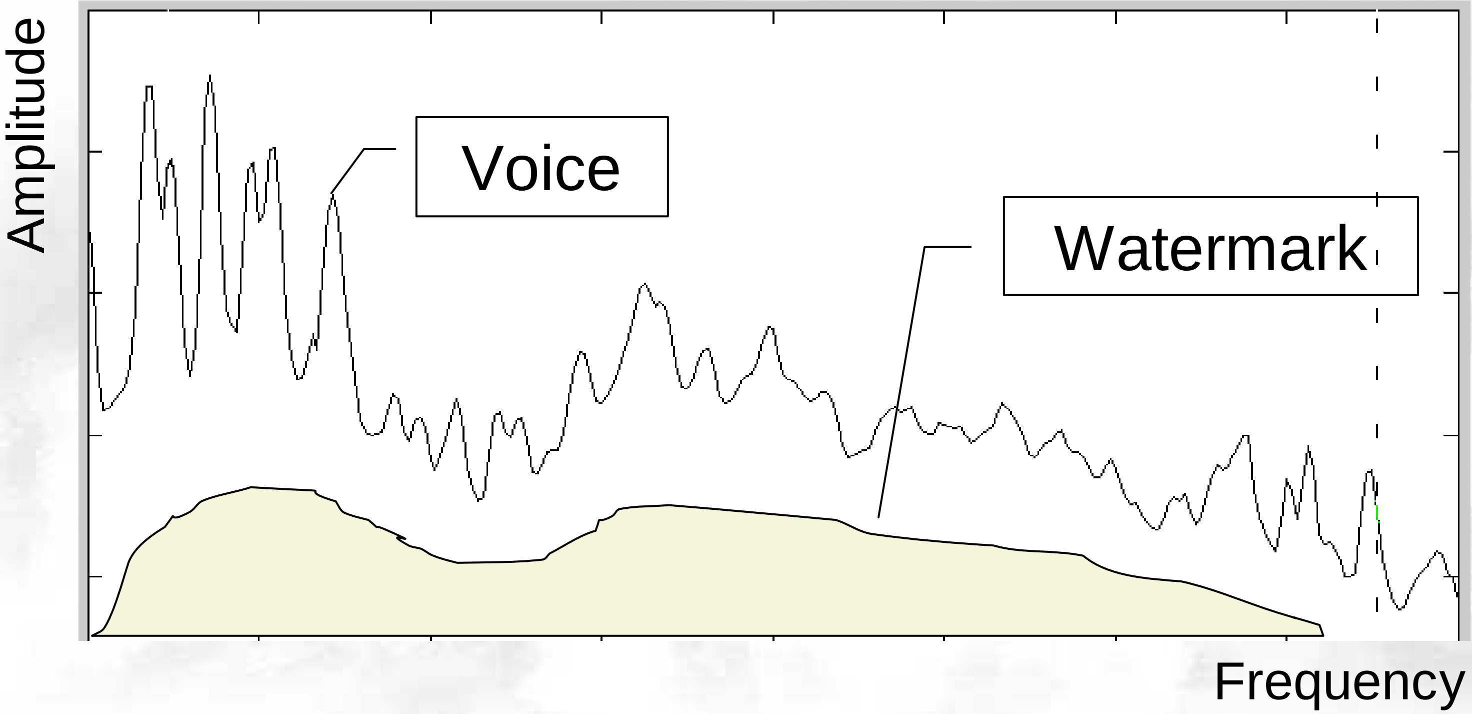


Watermark Embedders



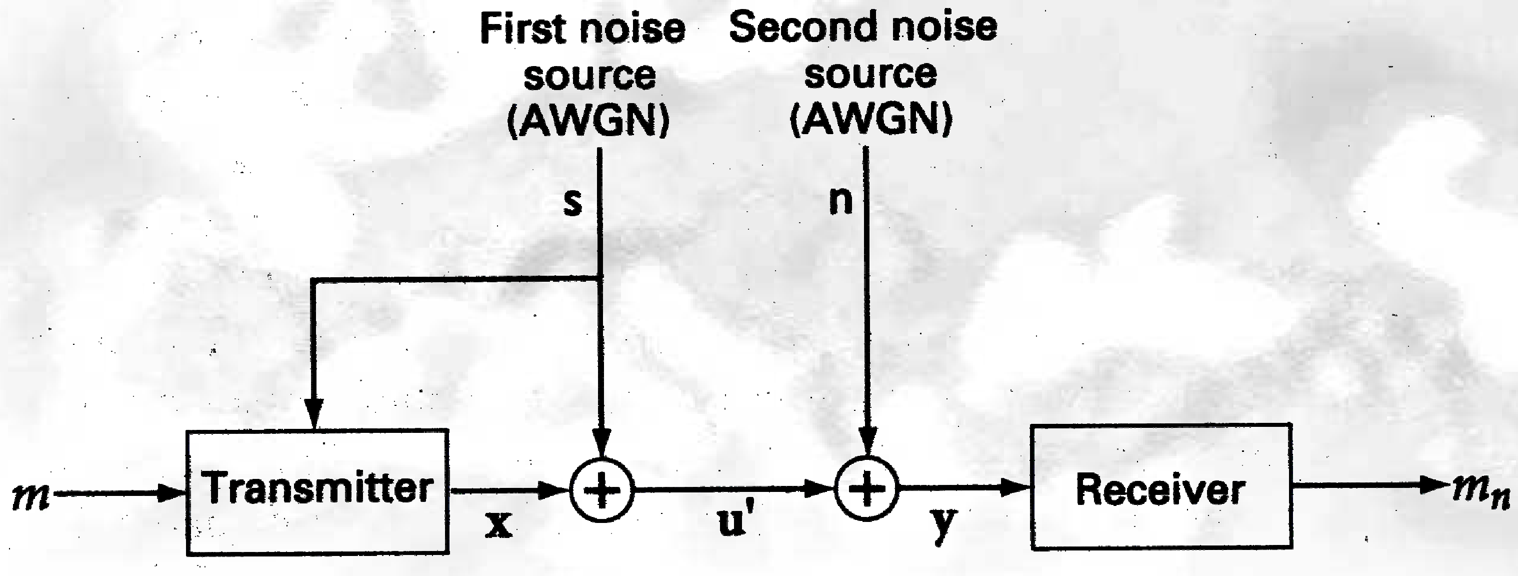
Spread Spectrum Techniques

“Aircraft Identification Tag” (AIT)



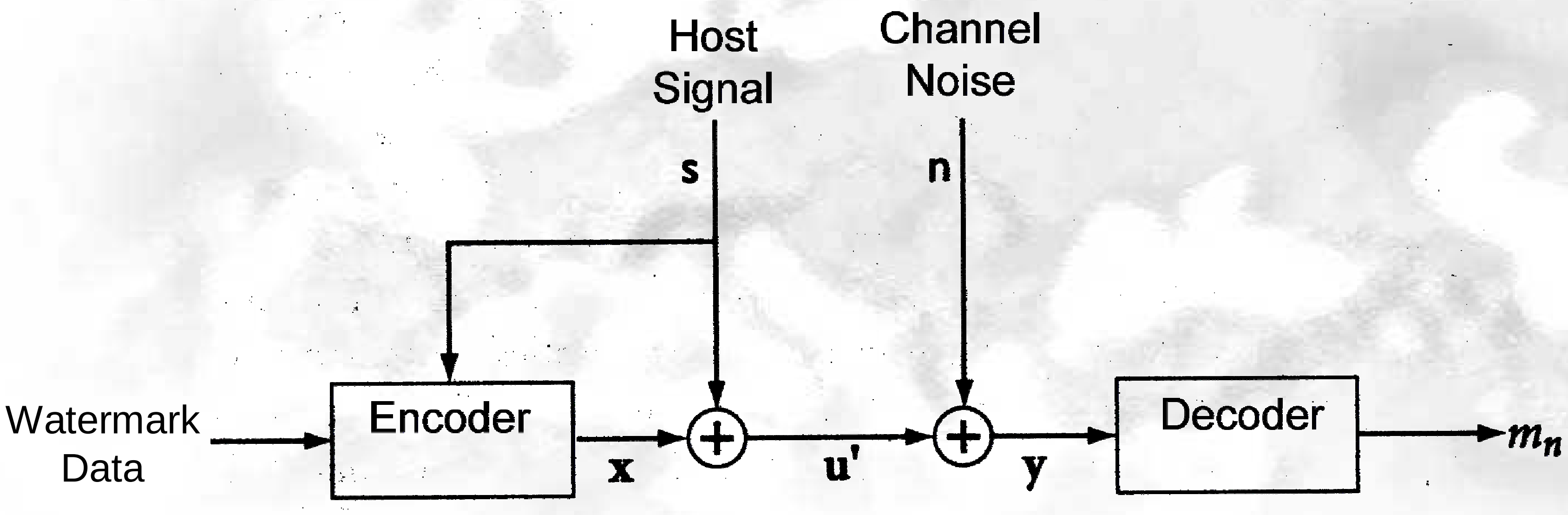
Known Host State Algorithms

- Communication over a channel with side information
- Costa’s “Dirty Paper Codes”



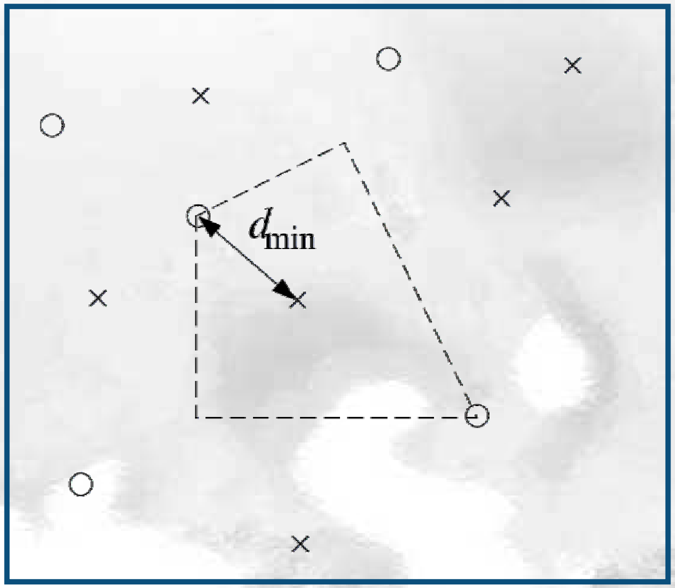
Known Host State Algorithms

- Communication over a channel with side information
- Costa's "Dirty Paper Codes"



Quantization Index Modulation (QIM-DC)

- Host signal as carrier
- Lattice (vector) coding
- Quantization of signal or its representation
- High capacity
- Issue: amplitude scaling



Robustness to Amplitude Scaling (Fading)

- ◆ Estimation of scaling at the decoder
  - ⇨ based on histogram of received signal
- ◆ Scaling-robust encoding
  - ➔ in transform domain
    - → cepstrum
    - → pitch of phonemes
    - → duration between glottal pulses
    - → …
  - ➔ with amplitude scaling robust codes
    - ⇨ modified Trellis codes
    - ⇨ correlation-based decoders

Conclusion

- ‘Digital’ features with legacy analogue radio
- Identification of sender
- Basis for
  - ➔ Speaker identification
  - ➔ Meta-tags for voice recordings
  - ➔ Adaptive channel equalization
  - ➔ Identification of locked aircraft transmitters
- Work in progress …

Digital Signatures for the Analogue Radio

Konrad Hofbauer
Graz University of Technology
Austria

konrad.hofbauer@eurocontrol.int

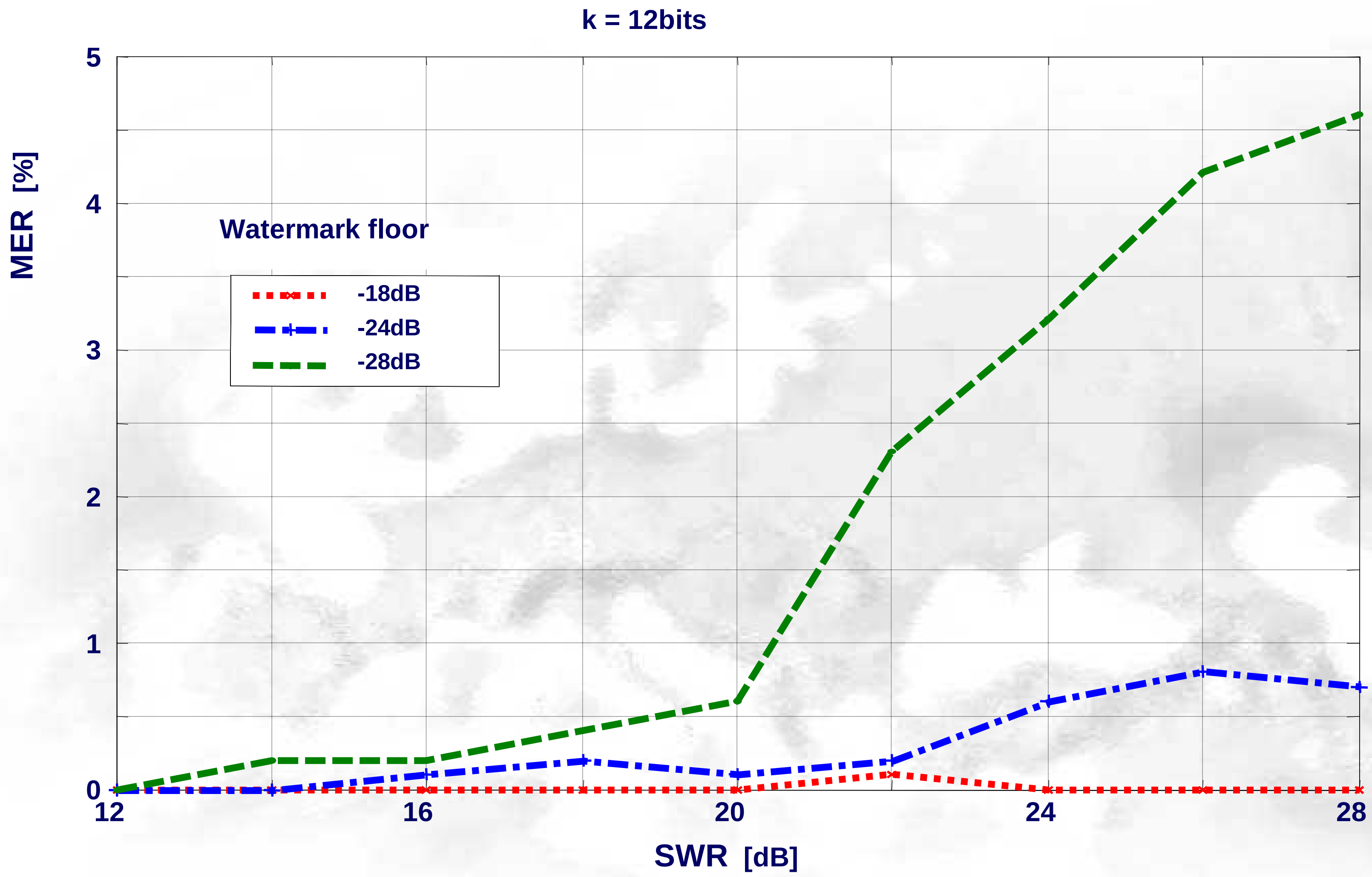
Horst Hering
Eurocontrol Experimental Centre
France

horst.hering@eurocontrol.int

EEC Actions for AIT

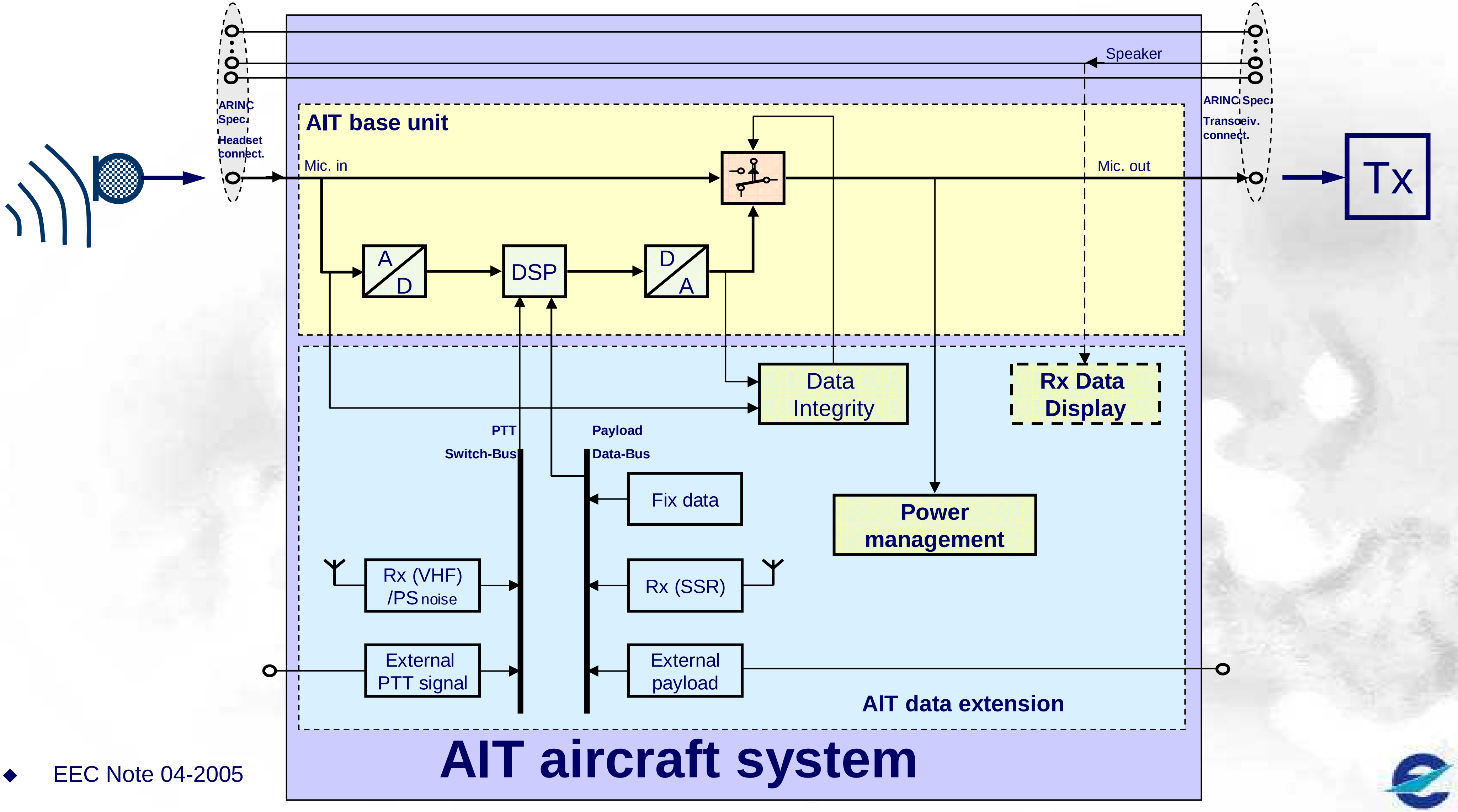
- **Research**
  - ⇨ Collaboration TUG - Ph.D. study K.Hofbauer
  - ⇨ Related research topics (data security, adaptive channel equalisation)
- **Flight tests**
  - ⇨ Collaboration University of Zilina, ….
- **Industrial co-operation to develop applications**
  - ⇨ Frequentis, Vienna
  - ⇨ Ruag, Interlaken
- **Project Evaluation (HQ)**
  - ⇨ Benefit analysis
  - ⇨ Stakeholder consultations

Results from TUG Experiments



- Data rate 80 bits/s; 12 bits payload data; watermark floor: –18db; 10^{-4} payload data error

AIT - Onboard Architecture



ARINC Spec. Headset connect.

ARINC Spec. Transceiv. connect.

Speaker

AIT base unit

Mic. in

Mic. out

Tx

A D

DSP

D A

Data Integrity

Rx Data Display

PTT Switch-Bus

Payload Data-Bus

Fix data

Power management

Rx (VHF) /PS noise

Rx (SSR)

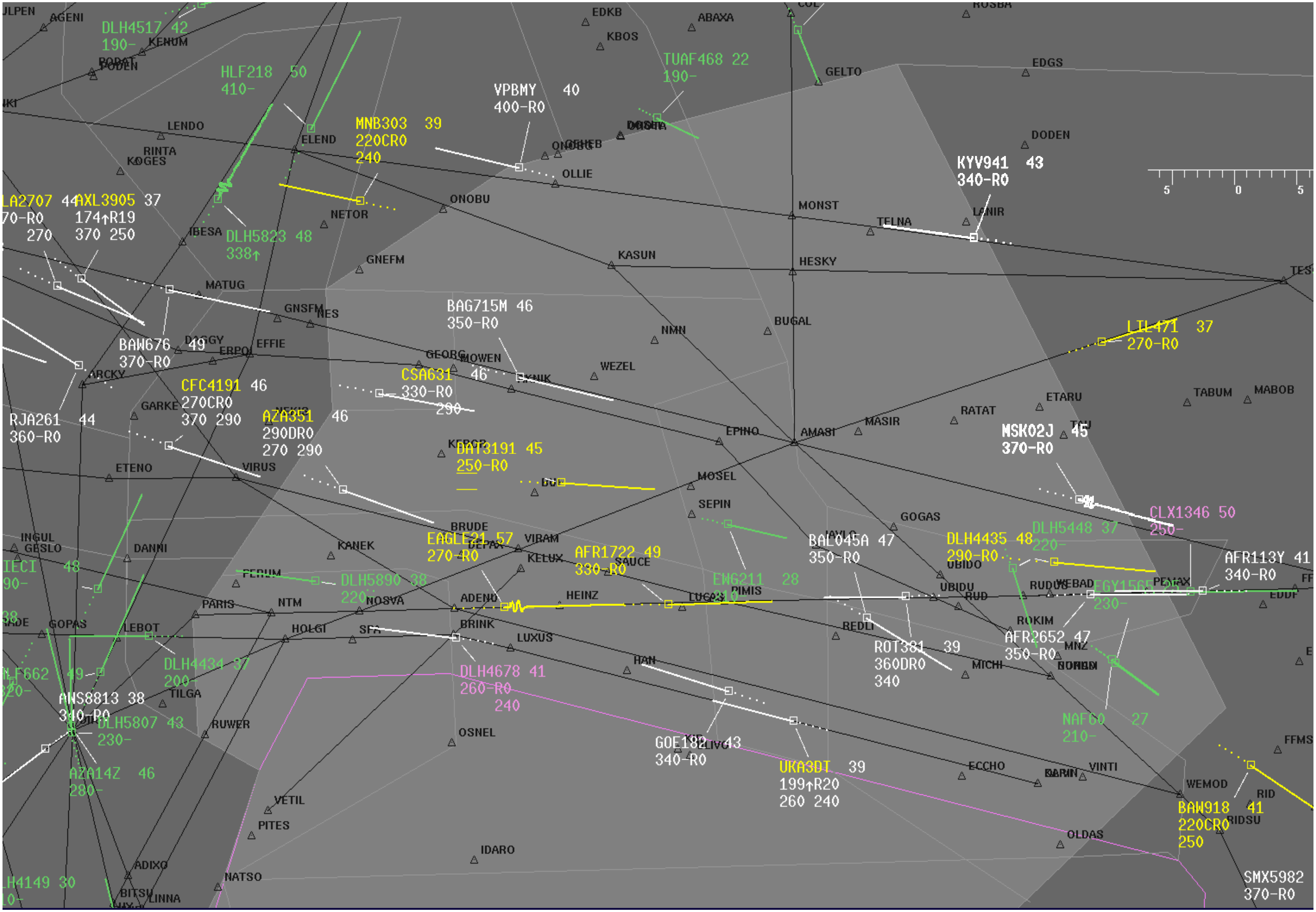
External PTT signal

External payload

AIT data extension

AIT aircraft system

- EEC Note 04-2005


ULPEN
AGENI
DLH4517 42
190-
KENUM
PODAT
PODEN
HLF218 50
410-
VPBMY 40
400-R0
EDKB
KBOS
ABAXA
TUAF468 22
190-
COL
GELTO
ROSBA
EDGS
DODEN
LENDO
RINTA
KOGES
ELEND
MNB303 39
220CR0
240
OLLIE
KYV941 43
340-R0
5
0
5
LA2707 44
70-R0
270
AXL3905 37
174↑R19
370 250
NETOR
ONOBU
MONST
TELNA
LANIR
IBESA
DLH5823 48
338↑
GNEFM
KASUN
HESKY
TES
MATUG
GNSFM
NES
BAG715M 46
350-R0
NMN
BUGAL
LIL471 37
270-R0
BAW676 49
370-R0
DAGGY
ERPOL
EFFIE
GEORG
MOWEN
WEZEL
ARCKY
CFC4191 46
270CR0
370 290
CSA631 46
330-R0
290
GARKE
AZA351 46
290DR0
270 290
TABUM
MABOB
ETARU
RATAT
RJA261 44
360-R0
MASIR
AMASI
EPINO
MSK02J 45
370-R0
KERPO
DAT3191 45
250-R0
ETENO
VIRUS
MOSEL
SEPIN
CLX1346 50
250-
GOGAS
INGUL
GESLO
DANNI
KANEK
BRUDE
EAGLE21 57
270-R0
VIBAM
DEPAX
KELUX
AFR1722 49
330-R0
SAUCE
BAL045A 47
350-R0
DLH4435 48
290-R0
DLH5448 37
220-
UBIDO
AFR113Y 41
340-R0
IECI 48
90-
PERUM
DLH5890 38
220
NOSVA
EWG211 28
210
PIMIS
LUCAS
UBIDU
RUDUS
RUD
WEBAD
FGY1565 25
230-
PEMAX
EDDF
38
ADE
GOPAS
LEBOT
PARIS
NTM
HOLGI
ADENU
HEINZ
BRINK
SFA
LUXUS
REDLI
ROT381 39
360DR0
340
ROKIM
AFR2652 47
350-R0
MNZ
NORED
MICHI
DLH4434 37
200-
LF662 49
320-
HAN
DLH4678 41
260-R0
240
ANS8813 38
340-R0
DLH5807 43
230-
TILGA
RUWER
OSNEL
GOE182 43
340-R0
LIVO
NAF60 27
210-
FFMS
AZA14Z 46
280-
UKA3DT 39
199↑R20
260 240
ECCHO
BARIN
VINTI
WEMOD
RID
VETIL
PITES
BAW918 41
220CR0
250
RIDSU
OLDAS
IDARO
ADIXO
NATSO
H4149 30
10-
BITSU
LINNA
SMX5982
370-R0